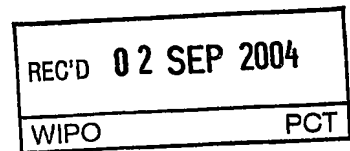


15. 7. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 7 月 1 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 2 7 5 6 7 2
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 2 7 5 6 7 2]

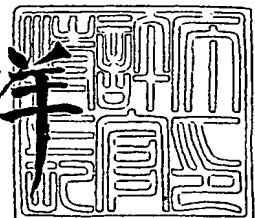
出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 8 月 1 9 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 2030750077
【提出日】 平成15年 7月16日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 15/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 高木 佳彦
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 菊地 隆文
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100105050
 【弁理士】
 【氏名又は名称】 鷺田 公一
【手数料の表示】
 【予納台帳番号】 041243
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9700376

【書類名】 特許請求の範囲**【請求項 1】**

機器からメモリデバイスに対するアクセス方法であって、
機器にて、
メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。

【請求項 2】

機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器にて、
前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。

【請求項 3】

機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、検証用鍵を共有化するステップと、
機器にて、
メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。

【請求項 4】

機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器とメモリデバイスとで、検証用鍵を共有化するステップと、
機器にて、
前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗

号化した検証データと、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。

【請求項 5】

機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器にて、
前記可能領域情報を参照し、第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。

【請求項 6】

機器からメモリデバイスに対するアクセス方法であって、
機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、
機器にて、
第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、
メモリデバイスにて、
前記指定情報を受信するステップと、
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、
前記検証にて成功した場合、前記処理命令を実行するステップと、
を有するアクセス方法。

【請求項 7】

機器からメモリデバイスに対するアクセス方法であって、
メモリデバイスは、
機器からのアクセスが制約された耐タンパ性の第 1 領域と、機器からのアクセスが制約された非耐タンパ性の第 2 領域と、機器からアクセスすることが可能な第 3 領域と、を有し、
少なくとも第 1 領域への処理命令である第一の処理系コマンドと、少なくとも第 3 領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、
機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、
機器にて、
前記可能領域情報を参照し、第二の処理系コマンドを用いて、第 2 領域へのアクセス領

域を指定する指定情報を送信するステップと、

第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、

メモリデバイスにて、

前記指定情報を受信するステップと、

前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、

前記検証にて成功した場合、前記処理命令を実行するステップと、

を有するアクセス方法。

【請求項 8】

機器からメモリデバイスに対するアクセス方法であって、

メモリデバイスは、

機器からのアクセスが制約された耐タンパ性の第 1 領域と、機器からのアクセスが制約された非耐タンパ性の第 2 領域と、機器からアクセスすることが可能な第 3 領域と、を有し、

少なくとも第 1 領域への処理命令である第一の処理系コマンドと、少なくとも第 3 領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、

機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、

機器にて、

第二の処理系コマンドを用いて、第 2 領域へのアクセス領域を指定する指定情報を送信するステップと、

第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、

メモリデバイスにて、

前記指定情報を受信するステップと、

前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、

前記検証にて成功した場合、前記処理命令を実行するステップと、

を有するアクセス方法。

【書類名】 明細書**【発明の名称】 アクセス方法****【技術分野】****【0001】**

本発明は、PCや携帯電話などの端末に挿入して使用されるメモリカードに対するアクセス方法に関するものである。

【背景技術】**【0002】**

従来、メモリカードは端末に挿入され、端末がデータを格納するためのものである。以下に、従来のメモリカードの一例をあげる。

【0003】

カードは、端末から各種コマンドを受け付け、またコマンドに対するレスポンスを返すコマンド用端子（CMDライン）と、データの入力を受け付け、またデータの出力を行うデータ用端子（DATライン）を持つ。

【0004】

図2に示したメモリカードの例では、端子22がCMDラインとなっており、端子27、28、29がDATラインであり、それぞれDAT0、DAT1、DAT2となっている。また端子21はデータ入出力用とカード検出用（CD）を兼ねたCD/DAT3となっている。DAT0～DAT3については、DAT0のみを使うモードと、DAT0～3を同時に利用しDAT0のみを使う場合の4倍の転送速度を実現するモードが存在する。

【0005】

次に、図3を用いて、従来カードのカード内モジュール構成について説明する。

【0006】

カード内モジュールは、コントローラ36とフラッシュメモリ35からなる。コントローラ36は、CMDラインに接続された、コマンド受信及びレスポンス送信を行うコマンド受信部31と、DATラインに接続されたデータ送受信部32と、フラッシュメモリ35へのデータの読み書きを行うメモリアクセス部34と、受信したコマンドに応じてデータの読み書き処理をメモリアクセス部に要求するデータ制御部33とからなる。

【0007】

次に、従来のメモリカードにおける、データ読み出し時の処理動作について説明する。ここではデータの出力はDAT0端子27のみを利用するモードに設定されているものとするが、DAT1端子28、DAT2端子29、DAT3端子21を併用するモードであってもよい。

【0008】

まず、端末はカードのCMDライン22にデータ読み出しコマンドを送信する。この読み出しコマンドは図4で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。データ読み出しコマンドにおけるコマンド引数は、読み出し開始アドレスを格納する。

【0009】

端末からコマンドを受信したコマンド受信部31は、コマンドコード401を参照して、データ読み出しコマンドであることを認識する。

【0010】

次に、コマンド受信部31は、コマンド引数402を参照して、指定されたアドレスが正しいものであるか、つまりカードが対応している範囲に指定されたアドレスが収まっているかを調べ、アドレスが正しくなければレスポンスとしてエラーである旨のレスポンスコードを返す。アドレスが正しければ正常である旨のレスポンスコードを返す。

【0011】

コマンド受信部31は、レスポンスを端末に返送した後、読み出しコマンドを受信したこと及び指定アドレスをデータ制御部33に伝える。

【0012】

データ制御部 33 は、メモリアクセス部 34 に対し、コマンド受信部 31 から受け取った指定アドレスとともに、読み出し要求を行う。

【0013】

メモリアクセス部 34 は、フラッシュメモリ 35 の指定アドレスからデータを読み出し、データ送受信部 32 に送信する。

【0014】

データ送受信部 32 は、DATA ライン 27 を通じて、端末に読み出しデータの出力を行う。

【0015】

このようなメモリカードでは、端末からアドレスを指定して自由にカードの読み書きが可能である。

【発明の開示】

【発明が解決しようとする課題】

【0016】

しかし、上記のようなメモリカードにおいて、フラッシュメモリの特定領域をセキュリティ保護領域としてアクセス制限をかけ、アクセスが許可された特定の端末からのみアクセス可能としたい場合、そのコマンド引数の小ささから柔軟な認証処理を行うことができない。

【0017】

例えば、コマンド引数にアクセス領域指定情報（アクセスするアドレスなど）と認証用の検証データを含める場合、アクセス領域に関する情報の長さが短くなればアクセス可能な領域が制限され、一方検証データの長さが短くなればセキュリティ強度が下がる。

【0018】

一方、コマンド形態を変更すると、メモリカードへのアクセスが複雑となり、端末にとっては利用しづらいものとなる。

【0019】

そこで本発明では、メモリカードコマンドと IC カードコマンドを併用し、メモリアクセスについてはメモリカードコマンドを使用することで複雑さを回避しながら、少ないコマンド引数でも安全に端末を認証可能なアクセス方法を提供することを目的とする。

【課題を解決するための手段】

【0020】

第 1 の発明は、機器からメモリデバイスに対するアクセス方法であって、機器にて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0021】

この発明によれば、引数の小さなメモリアクセス用コマンドにおいてアクセスを許可された端末を認証することが可能となる。

【0022】

第 2 の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器にて、前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0023】

この発明によれば、アクセス可能な領域を柔軟に設定可能となる。

【0024】

第3の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、検証用鍵を共有化するステップと、機器にて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0025】

この発明によれば、アクセスのたびに検証鍵を変更することでセキュリティ強度を上げることができる。

【0026】

第4の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器とメモリデバイスとで、検証用鍵を共有化するステップと、機器にて、前記可能領域情報を参照し、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0027】

この発明によれば、アクセス可能な領域を柔軟に変更するとともに、アクセス可能とした領域ごとに検証用鍵を設定することができる。

【0028】

第5の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器にて、前記可能領域情報を参照し、第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0029】

この発明によれば、アクセス可能な領域の共有を、メモリアクセス用コマンドとは異なるコマンド形態で行うことが可能となり、より柔軟な領域共有処理が可能となる。

【0030】

第6の発明は、機器からメモリデバイスに対するアクセス方法であって、機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、機器にて、第二の処理系コマンドを用いて、メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0031】

この発明によれば、検証鍵の共有を、メモリアクセス用コマンドとは異なるコマンド形態で行うことが可能となり、より柔軟な検証鍵共有処理が可能となる。

【0032】

第7の発明は、機器からメモリデバイスに対するアクセス方法であって、メモリデバイスは、機器からのアクセスが制約された耐タンパ性の第1領域と、機器からのアクセスが制約された非耐タンパ性の第2領域と、機器からアクセスすることが可能な第3領域と、を有し、少なくとも第1領域への処理命令である第一の処理系コマンドと、少なくとも第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、機器とメモリデバイスとで、第一の処理系コマンドを用いて、メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、機器にて、前記可能領域情報を参照し、第二の処理系コマンドを用いて、第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0033】

この発明によれば、端末からアクセスが制限された領域を、アクセス可能領域として共有可能となる。

【0034】

第8の発明は、機器からメモリデバイスに対するアクセス方法であって、メモリデバイスは、機器からのアクセスが制約された耐タンパ性の第1領域と、機器からのアクセスが制約された非耐タンパ性の第2領域と、機器からアクセスすることが可能な第3領域と、を有し、少なくとも第1領域への処理命令である第一の処理系コマンドと、少なくとも第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、機器とメモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、機器にて、第二の処理系コマンドを用いて、第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を関連付けて送信するステップと、メモリデバイスにて、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0035】

この発明によれば、端末からのアクセスが制限された領域が、カードとの間で検証用鍵を共有した端末からはアクセス可能となる。

【発明の効果】

【0036】

本発明は、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

【発明を実施するための最良の形態】

【0037】

本発明におけるカード内モジュール構成について図1を用いて説明する。なお、カードの端子構成は、図2に示したものと同様であるため、説明は省略する。

【0038】

カード内モジュールは、コントローラ106とフラッシュメモリ105からなる。コントローラ106は、CMDラインに接続された、コマンド受信及びレスポンス送信を行う

コマンド受信部101と、DATラインに接続されたデータ送受信部102と、フラッシュメモリ105へのデータの読み書きを行うメモリアクセス部104と、受信したコマンドに応じて、メモリアクセス部104、セッション鍵共有部110、及びパラメータ検証部108、暗復号部107に対して処理要求を行うデータ制御部103と、端末から受信したセキュリティ保護領域にアクセスするためのパラメータを記憶しておくパラメータ記憶部109と、パラメータが正しいことを検証するパラメータ検証部108と、端末との間で認証用及び暗復号用のセッション鍵を交換するセッション鍵共有部110と、セッション鍵と、セッション鍵と対応付けられたセキュリティ保護領域を記憶しておくエリア・セッション鍵管理部111からなる。

【0039】

端末とセッション鍵共有部110との間で送受信されるコマンド形態は、一般的なICカードで用いられるAPDU (Application Protocol Data Unit) フォーマットに従った形とする。つまり、セッション鍵共有部110はICカードアプリケーションの形態をとる。

【0040】

ここでは、APDUの送受信方法について説明する。

【0041】

まず、端末からカードに対するコマンドAPDUの送信処理について説明する。

【0042】

まず、端末はセッション鍵共有部110に対して送信するコマンドAPDUを作成する。次に、端末は図2のカードのCMDライン22に対して、APDU送信コマンドを送信する。

【0043】

このAPDU送信コマンドは、従来のデータ読み出しコマンドと同様、図4で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

【0044】

APDU送信コマンドにおけるコマンド引数402は、図14で示すように、DAT0ラインに入力するデータがコマンドAPDUであることを示すフラグ1401と送信データ数を示す1403とからなる。フラグ1401及び送信データ数1403を合わせて32ビットに満たない場合は未使用フィールド1402が存在する。

【0045】

図2のDAT0ライン27に入力するデータは512バイト単位となっており、送信データ数1403はこの512バイト単位の入力を何回行うかを示す。

【0046】

次に、カードのコマンド受信部101は、端末から送信されたコマンドを受信し、それがAPDU送信コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部103に対して、APDU送信コマンドを受信したことを通知する。

【0047】

次に、端末はカードのCMDライン22からAPDU送信コマンドに対するレスポンスを受信し、DAT0ライン27に図16で示すフォーマットでコマンドAPDU1602を入力する。

【0048】

図16において、1601で示される長さは後に続くAPDU1602の長さを示している。長さフィールド1601とAPDU1602の合計長にあわせてコマンド引数の送信データ数1403が設定されている。また、前記合計長は必ずしも512バイトの倍数になるわけではないので、512バイトの倍数になるようにパディング1603を付加する。

【0049】

次に、カード内部のデータ送受信部102は、端末から入力されたコマンドAPDUを

受信するとともに、データ制御部103にコマンドAPDUを受信したことを通知する。次に、データ制御部103は、データ送受信部101からコマンドAPDUを読み出し、セッション鍵共有部110（ICカードアプリケーション）にコマンドAPDUを渡す。

【0050】

次に、セッション鍵共有部110は、コマンドAPDUに記述されたとおりの処理を行い、処理の結果生じたデータとステータス情報をレスポンスAPDUとしてデータ制御部103に渡す。

【0051】

次に、カードから端末に対するレスポンスAPDUの送信処理について説明する。

【0052】

ここでは、前記のコマンドAPDUの送信方法で示したとおり、セッション鍵共有部110が出力したレスポンスAPDUがデータ制御部103で保持されている状態であるものとする。

【0053】

まず、端末は、カードのCMDライン22に対して、APDU受信コマンドを送信する。このAPDU受信コマンドは、APDU送信コマンドと同様、図4で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。APDU受信コマンドにおけるコマンド引数402は、図15で示すように、送信データ数を示す1502とからなる。送信データ数1502が32ビットに満たない場合は未使用フィールド1501が存在する。

【0054】

図2のDAT027から出力されるデータは、APDU送信コマンドにおける入力データと同様に512バイト単位となっており、送信データ数1502は512バイト単位で何回出力を行うかを示す。

【0055】

次に、カードのコマンド受信部101は、端末から送信されたコマンドを受信し、それがAPDU受信コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部103に対して、APDU受信コマンドを受信したことを通知する。

【0056】

次に、データ制御部103は、データ送受信部102に対して、セッション鍵共有部110から受け取ったレスポンスAPDUを渡す。

【0057】

次に、端末は、カードのCMDライン22からAPDU受信コマンドに対するレスポンスを受信し、DAT0ライン27からレスポンスAPDUを読み出す。読み出されるレスポンスAPDUは、図16で示すフォーマットで出力される。各フィールドの詳細については、APDU送信コマンドにおける入力時と同様であるため、説明を省略する。

【0058】

カードに搭載されるフラッシュメモリ105は、図6に示すように、少なくとも端末から従来の読み出し用コマンド及び書き込み用コマンドでアクセスすることが可能な通常領域62と、前記の従来のコマンドではアクセスすることができないセキュリティ保護領域61を持つ。

【0059】

セキュリティ保護領域61は、通常、カードアプリケーションからのみアクセス可能な状態であって、端末からの従来の読み出し用コマンド及び書き込み用コマンドに対しては、コマンド受信部101によってアクセスは排除される。

【0060】

本発明におけるメモリカードは内部に複数のカードアプリケーションを搭載することが可能となっており、図7のように、セキュリティ保護領域61は各アプリケーションに対して個別の領域（AP1用領域71～AP3用領域73）が割り当てられる。

【0061】

セキュリティ保護領域61は、データ制御部103が管理する格納用暗号鍵で暗号化されている。この暗号鍵は、セキュリティ保護領域61全体で1つのKsであってもよいし、各アプリケーション用のAP1用領域71～AP3用領域73に個別にKs__1～Ks__3を用意してもよい。本実施の形態では各アプリケーションAP1～3に格納用暗号鍵Ks__1～Ks__3を用意する。

【0062】

次に、セキュリティ保護領域61内の各アプリケーション用のAP1用領域71～AP3用領域73の内部構成について、図8を用いて説明する。

【0063】

ここでは、例としてカードアプリケーションAP1用領域71をあげている。AP1用領域71の内部はディレクトリDIR1、DIR2とファイルFILE1～FILE3を用いた階層構造を用いたデータ管理となっている。

【0064】

カードアプリケーションAP1は、AP1用領域71内でディレクトリ移動を行い、目的のファイルが存在するディレクトリDIR1、DIR2上でファイルFILE1～FILE3に対する読み書きを行う。

【0065】

例えば、カードアプリケーションAP1がファイルFILE3にアクセスする場合は、ディレクトリDIR1に移動し、次にディレクトリDIR2に移動した後、ファイルFILE3の読み書きを行う。また、各ディレクトリDIR1、DIR2において、その下位のディレクトリまたはファイルの作成及び削除が可能である。

【0066】

次に、カード内のセッション鍵共有部110と、端末との間で行われるセッション鍵共有手順について図9～図12を用いて説明する。

【0067】

カードアプリケーションと端末はそれぞれ公開鍵暗号で用いられる公開鍵と秘密鍵の対を保持し、お互いに相手の公開鍵を保持している。

【0068】

セッション鍵共有手順におけるコマンド形態は前記で示したAPDUを用いる。以降の説明においてはコマンド形態に関する記述を行わず、単にコマンド、レスポンスと表記する。

【0069】

まず、端末は、SELECTコマンドを送信することで、カードアプリケーションAP1の選択を行う（ステップ901）。

【0070】

カードは、端末から指定されたカードアプリケーションAP1の選択が正常に完了すれば正常完了のレスポンス、完了しなければ異常終了のレスポンスを返す（ステップ902）。

【0071】

次に、端末は、処理903を実行する。この処理903の詳細については、図10のフローチャートを参照して説明する。

【0072】

端末は、乱数Rhの生成を行い（ステップS9031）、乱数Rhと、端末がアクセスしたい図8で示したファイルFILE3のファイル名を結合し、カードアプリケーションAP1が保持する秘密鍵PriSに対応した公開鍵PubSで暗号化してDATA1を生成し（ステップS9032）、さらに端末が保持する秘密鍵PriHに対応した公開鍵PubHを示す識別子Info__PubHとDATA1を結合してDATA2を生成する（ステップS9033）。

【0073】

図9に戻り、次に、端末は、カードアプリケーションとのセッション鍵の共有及び、端

末がアクセス可能な領域情報の共有を行うために、ステップS9033で生成したDATA2を含んだREQ__AREA__INFOコマンドをカードアプリケーションに送信する(ステップ904)。

【0074】

REQ__AREA__INFOコマンドを受信したカードアプリケーションAP1は、処理905を実行する。この処理905の詳細については、図11のフローチャートを参照して説明する。

【0075】

カードアプリケーションAP1は、DATA2よりDATA1を抽出し、カードアプリケーションAP1が保持する秘密鍵PriSで復号化し、乱数Rhとファイル名FILE3を得る(ステップS9051)。

【0076】

次に、DATA2より公開鍵を識別して識別子Info__PubHを抽出し、Info__PubHが示す公開鍵PubHに対応付けられた端末がファイルFILE3にアクセスする権限があるかを確認する。権限がなければ、その旨のエラーをレスポンスとして端末に返す。アクセスする権限があれば、FILE3のファイルサイズSIZE3を取得する(ステップS9052)。

【0077】

次に、乱数Rsを生成し(ステップS9053)、ファイルFILE3を端末からアクセス可能となるように設定を行い、端末がアクセスするとき使用するためのエリア番号XをファイルFILE3に割り当て、ファイルサイズSIZE3とともにエリア・セッション鍵管理部111に記憶する(ステップS9054)。

【0078】

次に、乱数Rs、エリア番号X、ファイルサイズSIZE3を結合し、DATA3を生成し(ステップS9055)、DATA3を端末の公開鍵PubHで暗号化してDATA4を生成する(ステップS9056)。

【0079】

次に、乱数Rsと乱数Rhに排他的論理和を施し、乱数Rを生成し(ステップS9057)、乱数Rから暗号用セッション鍵Kd、検証用セッション鍵Kmを生成する(ステップS9058)。

【0080】

次に、セッション鍵Kd及びKmをエリア番号Xと関連付け、エリア・セッション鍵管理部111に記憶する(ステップS9059)。

【0081】

図9に戻り、カードはここまでの処理を終えると端末にDATA4を含んだレスポンスAPDUを端末に送信する(ステップ906)。

【0082】

レスポンスAPDUを受信した端末は、処理907を実行する。この処理907の詳細については、図12のフローチャートを参照して説明する。

【0083】

端末は、端末の秘密鍵PriHを用いてDATA4を復号しDATA3を取得する(ステップS9071)。次に、端末は、DATA3より乱数Rsを取得し、乱数Rsと乱数Rhに排他的論理和を施し、乱数Rを生成し(ステップS9072)、乱数Rから暗号用セッション鍵Kd、検証用セッション鍵Kmを生成する(ステップS9073)。

【0084】

以上のステップ901から907を踏むことで、端末とカード間の相互認証を行い、かつ端末が指定したファイルに対するアクセス権限があれば端末からのアクセスが可能な状態となり、またアクセスする際に必要なエリア番号、エリア番号に割り当てられたファイルのサイズ、および検証用セッション鍵、暗号用セッション鍵を共有することができる。

【0085】

なお、ステップ904において端末からカードに伝えられるファイル名は、カードアプリケーションが管理するファイルを直接示すものである必要はなく、カードアプリケーションがどのファイルを指しているかが認識できる形であればよい。

【0086】

また、端末がアクセスしたいファイル及びステップS9054において、そのファイルに対して端末がアクセス可能となる設定を行った際に割り当てられるエリア番号が常になるとなるようにし、これらの情報を端末とカード間であらかじめ認識しておくことで、ステップ904における端末がアクセスしたいファイル名の通知およびステップ906におけるファイルに割り当てられたエリア番号の通知を省略することもできる。

【0087】

さらに、本説明では、各カードアプリケーションが図8で示すようにディレクトリとファイルからなる階層構造をもち、ディレクトリ名およびファイル名でデータを管理している形態で説明したが、カードアプリケーションに割り当てられた領域を適当な大きさに分割し、分割されたそれぞれの領域に番号のような識別子を割り当てて管理する形態でもよい。その場合は、図9で示した処理手順で用いられるファイル名FILE3の代わりに前記識別子を用いる。

【0088】

次に、端末からセキュリティ保護領域に対してアクセスを行う際の処理について図13及び図1を用いて説明する。

【0089】

まず、端末はカードに対してアクセス領域指定コマンドを送信する（ステップ1301）。このアクセス領域指定コマンドは、APDU送信コマンドと同様、図4で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

【0090】

アクセス領域指定コマンドにおけるコマンド引数402は、図14で示すように、DAT0ライン27に入力するデータがアクセス領域指定情報であることを示すフラグ1401と送信データ数を示す1403とからなる。フラグ1401及び送信データ数1403を合わせて32ビットに満たない場合は未使用フィールド1402が存在する。

【0091】

DAT0ライン27に入力するデータは、512バイト単位となっており、送信データ数1403は、この512バイト単位の入力を何回行うかを示す。

【0092】

次に、カードのコマンド受信部101は、端末から送信されたコマンドを受信し、それがアクセス領域指定コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部103に対して、アクセス領域指定コマンドを受信したことを通知する（ステップ1302）。

【0093】

次に、端末はカードのCMDライン22からアクセス領域指定コマンドに対するレスポンスを受信し、DAT0ライン27に図17で示すフォーマットでアクセス領域指定情報1702を入力する（ステップ1303）。

【0094】

図17の1701で示される長さは、後に続くアクセス領域指定情報1702の長さを示している。長さフィールド1701とアクセス領域指定情報1702の合計長に合わせてコマンド引数402の送信データ数1403が設定されている。また、前記合計長は必ずしも512バイトの倍数になるわけではないので、512バイトの倍数になるようにパディング1703を付加する。

【0095】

アクセス領域指定情報1702は、図18で示されるように、図9のステップ906でカードから通知されたエリア番号Xを指定するエリア番号1801と、0～同じくカード

から通知されたファイルサイズ SIZE 3 の範囲で選択可能なアクセス開始アドレス 1802 と、1 ～ (ファイルサイズ SIZE 3 - アクセス開始アドレス 1802) の範囲で選択可能なアクセスデータサイズ 1803 とで構成される。

【0096】

次に、カード内部のデータ送受信部 102 は、端末から入力されたアクセス領域指定情報 1702 を受信するとともに、データ制御部 103 にアクセス領域指定情報 1702 を受信したことを通知する。

【0097】

次に、データ制御部 103 は、データ送受信部 102 からアクセス領域指定情報 1702 を読み出し、エリア番号 1801 が、図 11 のステップ S9054 にて割り当てられたエリア番号 X であるか、アクセス開始アドレス及びアクセスデータサイズは、エリア番号 X と対応したファイルのファイルサイズ範囲に収まっているかをチェックし、異常があればエラーフラグを設定する。

【0098】

データ制御部 103 は、異常がなければ、図 1 に示すパラメータ記憶部 109 にアクセス領域指定情報 1702 を記憶する。

【0099】

以上が、アクセス領域を指定する処理である。

【0100】

次に、図 6 のセキュリティ保護領域 61 に対して読み出しを行う際の処理について説明する。

【0101】

図 13 において、端末は、カードに対してセキュリティ保護領域読み出しコマンドを送信する(ステップ 1304)。このセキュリティ保護領域読み出しコマンドは、APDU 送信コマンドと同様、図 4 で示されるフォーマットとなっており、6 ビットのコマンドコード 401 と 32 ビットのコマンド引数 402 から構成される。

【0102】

セキュリティ保護領域読み出しコマンドにおけるコマンド引数 402 は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末と同一であるか、またセッション鍵共有手順を経てエリア番号 X が示す領域に対するアクセス権限があることを確認された端末と同一であるかを検証するための検証データからなる。

【0103】

この検証データの生成方法について図 5 を用いて説明する。

【0104】

アクセス領域指定情報 1702 は、アクセス領域指定コマンドにおいて DAT ラインに入力するパラメータである。検証鍵 501 は、図 9 のステップ 907 で生成した検証用セッション鍵 Km である。

【0105】

検証データ作成部 503 は、暗号演算を行うモジュールである。ここでは、DES-MAC と呼ばれる MAC 生成処理を行う。アクセス領域指定情報 1702 に対してパディングデータ 505 を付加した 502 を入力データとして、検証鍵 501 を用いて DES 暗号を用いた MAC 生成処理を行い、検証データとして MAC データ 504 を作成する。

【0106】

パディングデータ 505 については、端末からカードに対してアクセス領域指定コマンドを送信するときにアクセス領域指定情報 1702 と併せて送信してもよいし、あらかじめ端末とカードの間で取り決めをしたパディング生成ルールに基づいて生成したパディングデータを付与してもよい。

【0107】

なお、本実施の形態では DES-MAC を用いて検証データを作成しているが、他のア

ルゴリズムを用いてもよい。

【0108】

なお、端末が正当であるか認証する必要がなく、アクセス領域指定コマンドとの対応付けのみ確認したい場合は、暗号処理を用いずに、単にSHA1やMD5アルゴリズムを用いたハッシュデータを検証データとして用いてもよい。

【0109】

端末は、上記の検証データ生成処理によって32ビットの検証データを生成し、セキュリティ保護領域読み出しコマンドの引数として使用する。

【0110】

次に、カードのコマンド受信部101は、端末から送信されたコマンドを受信し、それがセキュリティ保護領域読み出しコマンドであることを認識し、アクセス領域指定情報1702に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。また、アクセス領域指定情報1702に関するエラーフラグが設定されていない場合は、図13で示すように、端末に正常レスポンスを返す(ステップ1305)とともに、データ制御部103に対してセキュリティ保護領域読み出しコマンドを受信したことを通知し、パラメータ検証部108にコマンド引数402として与えられた検証データ504を渡す。

【0111】

次に、端末は、カードのCMDライン22からセキュリティ保護領域読み出しコマンドに対するレスポンスを受信し、DAT0ライン27からデータが出力されるのを待つ。

【0112】

以降にカードによるセキュリティ保護領域のデータ出力処理について説明する。

【0113】

カードのパラメータ検証部108は、パラメータ記憶部109からアクセス領域指定コマンドによって端末から与えられ、記憶しておいたアクセス領域指定情報1702を読み出し、アクセス領域指定情報1702に含まれるエリア番号X(1801)に対応する、図11のステップS9059で記憶した検証用セッション鍵Kmをエリア・セッション鍵管理部111から取得する。

【0114】

次に、カードのパラメータ検証部108は、検証用セッション鍵Kmとアクセス領域指定情報1702を用いて、図19に示した検証データ生成処理を行い、検証データ1904を生成する。なお、検証データ生成処理については、図5で示した端末による検証データ生成処理と同様であるので詳細な説明は省略する。

【0115】

次に、カードのパラメータ検証部108は、上記検証データ生成処理で生成した検証データ1904と、端末からセキュリティ保護領域読み出しコマンドの引数によって与えられた検証データ504を比較し、一致しなければエラーとし、データ読み出し処理に移行しない。一致した場合は、次のデータ読み出し処理に移行することをデータ制御部103に通知する。

【0116】

次に、カードのデータ制御部103は、パラメータ記憶部109からアクセス領域指定情報1702を読み出し、その中に含まれるエリア番号Xを取得し、エリア・セッション鍵管理部111からエリア番号に対応するファイルFILE3を認識する。

【0117】

次に、カードのデータ制御部103は、ファイルFILE3がアプリケーションAP1用の領域であることを確認し、格納用暗号鍵Ks_1を取得する。

【0118】

次に、カードのデータ制御部103は、アクセス領域指定情報1702からアクセス開始アドレス1802とアクセスデータサイズ1803を取得し、ファイルFILE3として管理されている領域に対して、アクセス開始アドレス1802をオフセット、アクセス

データサイズ 1 8 0 3 を読み出しサイズとしてメモリアクセス部 1 0 4 にデータ読み出し要求を行う。

【0 1 1 9】

次に、カードのデータ制御部 1 0 3 は、暗復号部 1 0 7 に対して、メモリアクセス部 1 0 4 によって読み出されたデータを格納用暗号鍵 K s _ 1 で復号化するように要求する。

【0 1 2 0】

次に、カードのデータ制御部 1 0 3 は、暗復号部 1 0 7 に対して、暗復号部 1 0 7 によって復号化されたデータを暗号用セッション鍵 K d で暗号化するように要求する。

【0 1 2 1】

次に、カードのデータ制御部 1 0 3 は、データ送受信部 1 0 2 に対して、暗復号部 1 0 7 によって暗号用セッション鍵 K d で暗号化されたデータを端末に送信するように要求する。

【0 1 2 2】

上記の処理によって、カードからセキュリティ保護領域のデータがセッション鍵 K d によって暗号化された状態で出力可能となる。

【0 1 2 3】

端末は、カードからデータが出力可能となったことを認識し、図 1 3 に示すように、D A T 0 ライン 2 7 からセッション鍵 K d によって暗号化された状態のデータを取得し（ステップ 1 3 0 6）、端末が保持する暗号用セッション鍵 K d によってデータを復号化し、アクセス領域指定情報 1 7 0 2 で指定した領域のデータを得る。

【0 1 2 4】

次に、セキュリティ保護領域に対して書き込みを行う際の処理について、図 2 0 を参照して説明する。

【0 1 2 5】

端末は、カードに対してセキュリティ保護領域書き込みコマンドを送信する（ステップ 2 0 0 4）。このセキュリティ保護領域書き込みコマンドは、A P D U 送信コマンドと同様、図 4 で示されるフォーマットとなっており、6 ビットのコマンドコード 4 0 1 と 3 2 ビットのコマンド引数 4 0 2 から構成される。

【0 1 2 6】

セキュリティ保護領域読み出しコマンドにおけるコマンド引数 4 0 2 は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末と同一であるか、またセッション鍵共有手順を経てエリア番号 X が示す領域に対するアクセス権限があることを確認された端末と同一であることを検証するための検証データ 1 9 0 4 からなる。

【0 1 2 7】

この検証データの生成方法についてはセキュリティ保護領域読み出しコマンドと同様であるため、詳細な説明は省略する。

【0 1 2 8】

端末は、検証データ生成処理によって 3 2 ビットの検証データを生成し、セキュリティ保護領域書き込みコマンドの引数として使用する。

【0 1 2 9】

次に、カードのコマンド受信部 1 0 1 は、端末から送信されたコマンドを受信し、それがセキュリティ保護領域書き込みコマンドであることを認識し、アクセス領域指定情報 1 7 0 2 に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。

【0 1 3 0】

また、アクセス領域指定情報 1 7 0 2 に関するエラーフラグが設定されていない場合は、端末に正常レスポンスを返す（ステップ 2 0 0 5）とともに、データ制御部 1 0 3 に対してセキュリティ保護領域書き込みコマンドを受信したことを通知し、パラメータ検証部 1 0 8 にコマンド引数として与えられた検証データ 5 0 4 を渡す。

【0 1 3 1】

次に、端末は、カードのCMDライン22からセキュリティ保護領域書き込みコマンドに対するレスポンスを受信し、DAT0ライン27にデータの入力を行う（ステップ2006）。ここでDAT0ライン27に入力するデータは、図9のステップ907で生成した暗号用セッション鍵Kdで暗号化したものである。また、入力データサイズは、アクセス領域指定情報1702で指定したアクセスデータサイズと同一である。

【0132】

以降にカードによるセキュリティ保護領域へのデータ格納処理について説明する。

【0133】

カードのパラメータ検証部108は、パラメータ記憶部109からアクセス領域指定コマンドによって端末から与えられ、記憶しておいたアクセス領域指定情報1702を読み出し、アクセス領域指定情報1702に含まれるエリア番号X（1801）に対応する、図11のステップ9059で記憶した検証用セッション鍵Kmをエリア・セッション鍵管理部111から取得する。

【0134】

次に、カードのパラメータ検証部108は、検証用セッション鍵Kmとアクセス領域指定情報1702を用いて、図19に示した検証データ生成処理を行い、検証データ1904を生成する。なお、検証データ生成処理については、図5で示した端末による検証データ生成処理と同様であるので詳細な説明は省略する。

【0135】

次に、カードのパラメータ検証部108は、上記で生成した検証データ1904と、端末からセキュリティ保護領域書き込みコマンドの引数によって与えられた検証データ504を比較し、一致しなければエラーとし、データ書き込み処理に移行しない。一致した場合は次のデータ書き込み処理に移行することをデータ制御部103に通知する。

【0136】

次に、カードのデータ制御部103は、パラメータ記憶部109からアクセス領域指定情報1702を読み出し、その中に含まれるエリア番号Xを取得し、エリア・セッション鍵管理部111からエリア番号に対応するファイルFILE3を認識する。

【0137】

次に、カードのデータ送受信部102は、端末から入力されたデータを受信する。

【0138】

次に、カードのデータ制御部103は、ファイルFILE3がアプリケーションAP1用の領域であることを確認し、格納用暗号鍵Ks__1を取得する。

【0139】

次に、カードのデータ制御部103は、暗復号部107に対して、データ送受信部102が受信したデータを暗号用セッション鍵Kdで復号化するよう要求する。

【0140】

次に、カードのデータ制御部103は、暗復号部107に対して、暗復号部107が復号化したデータを格納用暗号鍵Ks__1で暗号化するよう要求する。

【0141】

次に、カードのデータ制御部103は、アクセス領域指定情報1702からアクセス開始アドレス1802とアクセスデータサイズ1803を取得し、ファイルFILE3として管理されている領域に対し、アクセス開始アドレス1802をオフセット、アクセスデータサイズ1803を書き込みサイズとして、メモリアクセス部104に対してデータ書き込み要求を行う。

【0142】

上記のようにして、端末が入力したセッション鍵Kdで暗号化されたデータを格納鍵Ks__1で暗号化してフラッシュメモリに格納する。

【0143】

本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報の共有を1つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

【0144】

本実施の形態では、図9にてセッション鍵共有手順を含めているが、セキュリティポリシーとしてセッション鍵を毎回更新する必要がないと考える場合は、端末およびカードがあらかじめ検証鍵および暗号鍵を保持し、それをセッション鍵として用いてもよい。

【0145】

以上、本発明のように、ICカード用コマンドとメモリアクセス用コマンドを受信可能なメモリカードにおいて、カードアプリケーションが利用し、通常はカードアプリケーション経由でのみアクセス可能であり、端末からのアクセスが制限されているセキュリティ保護領域に対して、カードアプリケーションと端末が相互認証し、カードアプリケーションがアクセス可能設定を行うことにより、端末からメモリアクセス用コマンドを用いてアクセスすることが可能となる。

【0146】

また、カードアプリケーションがアクセス可能設定を行うためのカードアプリケーションと端末間の相互認証は、用途が限定されたメモリアクセス用コマンドではなく、ICカード用コマンドを使うことにより、データのセキュリティレベルに応じて相互認証方式を柔軟に選択可能となる。

【0147】

また、メモリアクセス用コマンドに含められる引数サイズが32ビットのように小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

【0148】

また、検証用及び暗号用セッション鍵の共有処理をセキュリティ保護領域アクセスのたびに行うことにより、セキュリティ保護領域アクセスに含める検証データとして適当な値を設定して繰り返し不正アクセスを行う攻撃に対する防御性を高めることができる。

【0149】

また、端末からアクセスしたいファイルをカードに通知し、それにエリア番号を割り当て、カードから端末に通知することにより、端末がアクセス可能な領域を設定することが可能となる。また、複数のファイルに対して行うことにより、同時に複数のファイルに対してアクセス可能な状態を作ることができる。

【産業上の利用可能性】

【0150】

本発明にかかるアクセス方法は、メモリカードコマンドとICカードコマンドを併用し、メモリアクセスについてはメモリカードコマンドを使用することで複雑さを回避しながら、少ないコマンド引数でも安全に端末を認証可能とすることである。

【図面の簡単な説明】

【0151】

【図1】本発明の一実施の形態におけるメモリカードの内部モジュール構成を示す図

【図2】カードの端子を示す図

【図3】従来のメモリカードの内部モジュール構成を示す図

【図4】本実施の形態におけるメモリカードのコマンドフォーマットを示す図

【図5】本実施の形態における端末の正当性検証を行うための検証データの端末による生成方法を示す図

【図6】本実施の形態におけるフラッシュメモリの内部構成を示す図

【図7】本実施の形態におけるセキュリティ保護領域の内部構成を示す図

【図8】本実施の形態におけるセキュリティ保護領域内の各アプリケーション用領域の内部構成を示す図

【図9】本実施の形態におけるセッション鍵共有及びアクセス可能領域共有手順を示

す図

【図 10】 図 9 のステップ 903 における処理の詳細を説明するためのフローチャート

【図 11】 図 9 のステップ 905 における処理の詳細を説明するためのフローチャート

【図 12】 図 9 のステップ 907 における処理の詳細を説明するためのフローチャート

【図 13】 本実施の形態における端末からセキュリティ保護領域を読み出すためのコマンドシーケンスを示す図

【図 14】 本実施の形態における APDU 送信コマンドの引数フォーマットを示す図

【図 15】 本実施の形態における APDU 受信コマンドの引数フォーマットを示す図

【図 16】 本実施の形態における APDU 送信コマンドの入力データ及び APDU 受信コマンドの出力データのフォーマットを示す図

【図 17】 本実施の形態におけるアクセス領域指定コマンドの入力データフォーマットを示す図

【図 18】 本実施の形態におけるアクセス領域指定情報を示す図

【図 19】 本実施の形態における端末の正当性検証を行うための検証データのカードによる生成方法を示す図

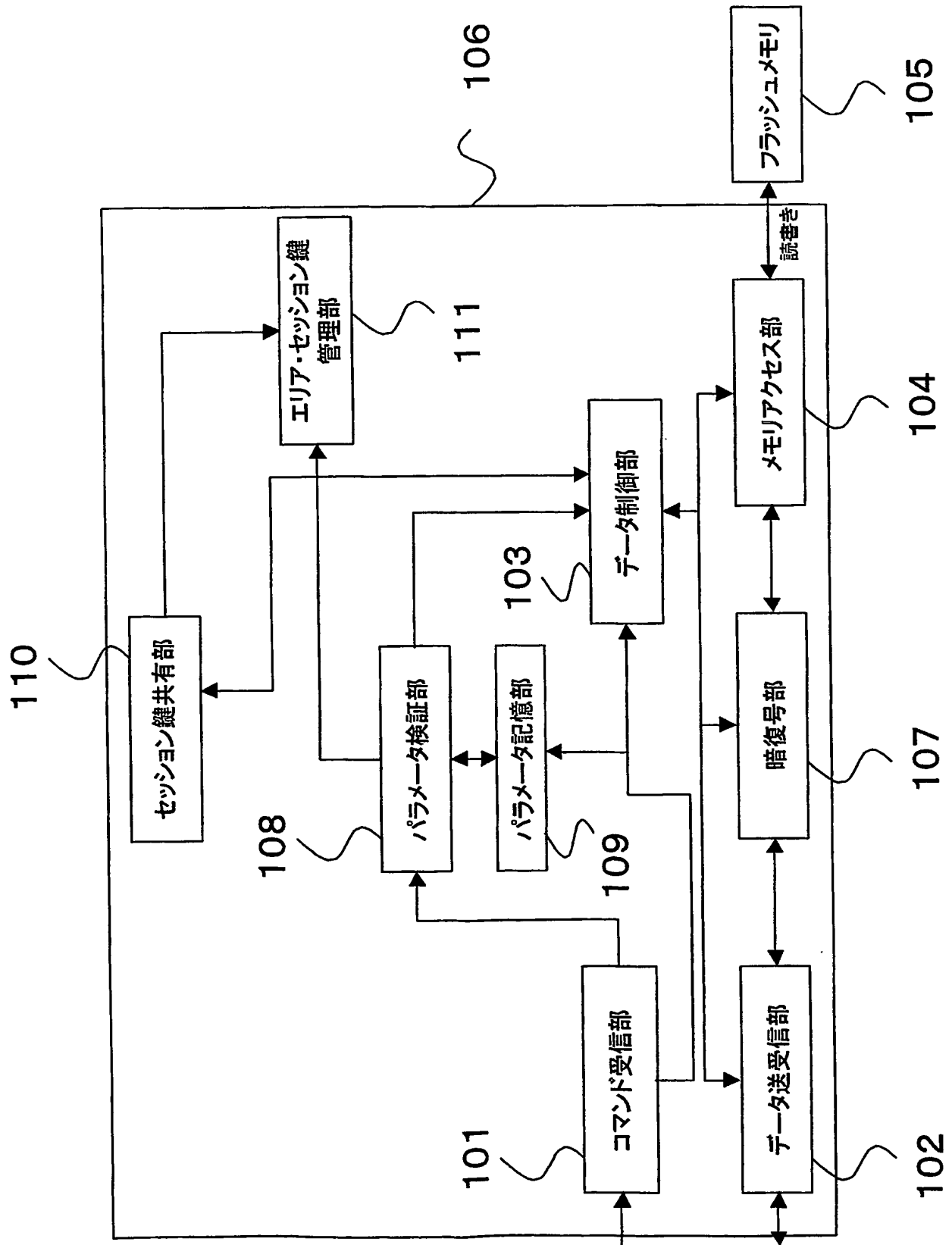
【図 20】 本実施の形態における端末からセキュリティ保護領域に書き込むためのコマンドシーケンスを示す図

【符号の説明】

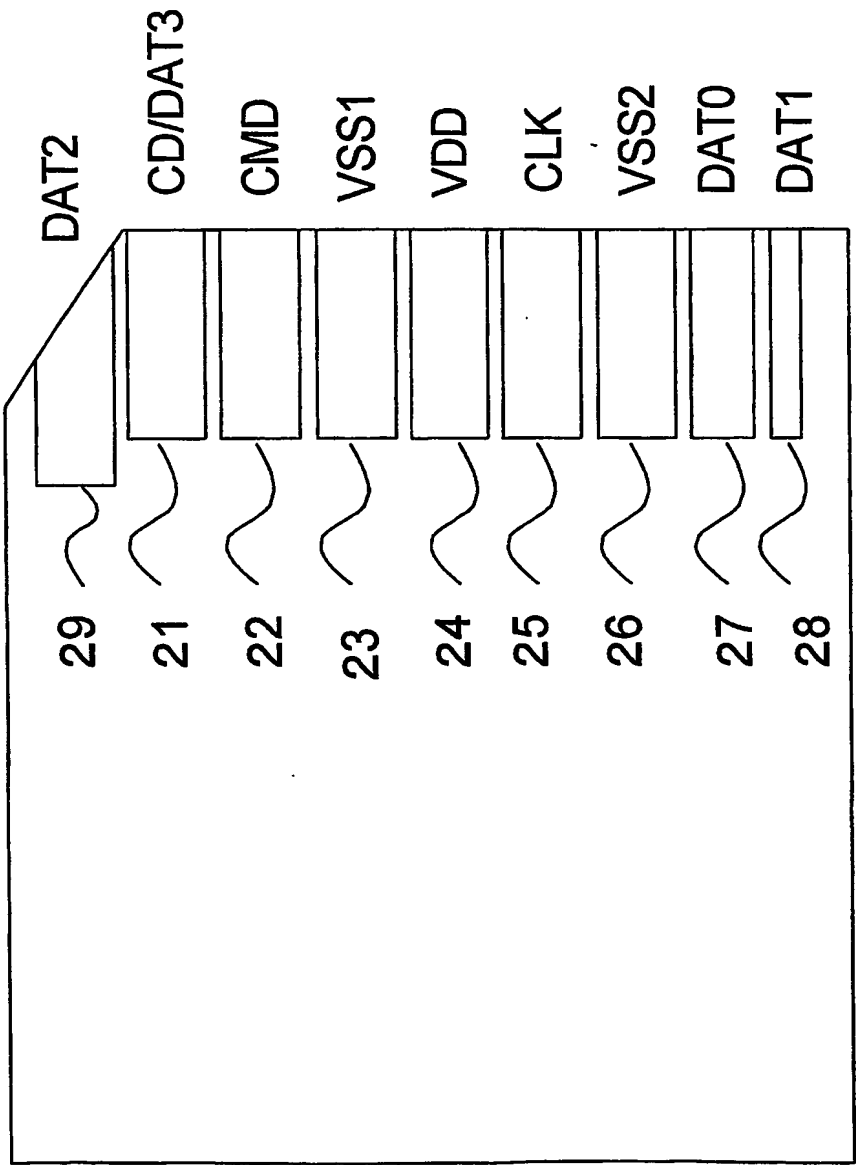
【0152】

- 101 コマンド受信部
- 102 データ送受信部
- 103 データ制御部
- 104 メモリアクセス部
- 105 フラッシュメモリ
- 106 コントローラ
- 107 暗復号部
- 108 パラメータ検証部
- 109 パラメータ記憶部
- 110 セッション鍵共有部
- 111 エリア・セッション鍵管理部

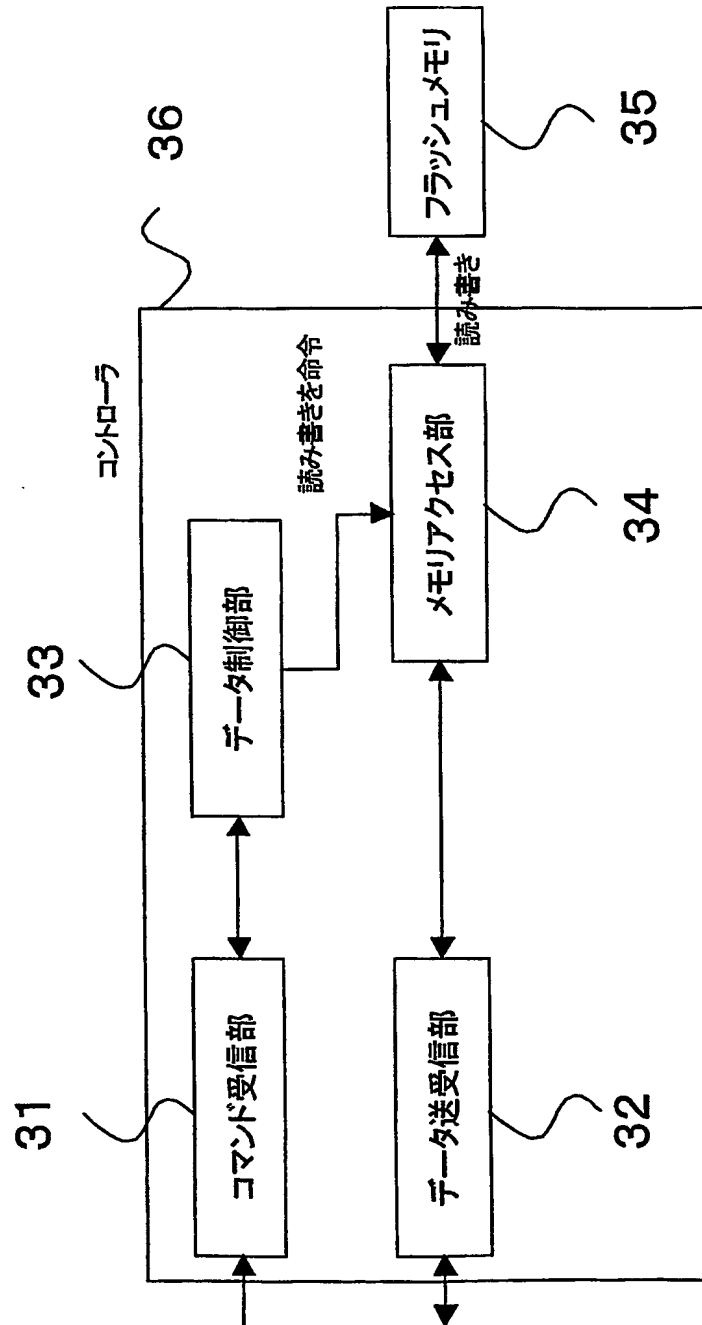
【書類名】 図面
【図1】



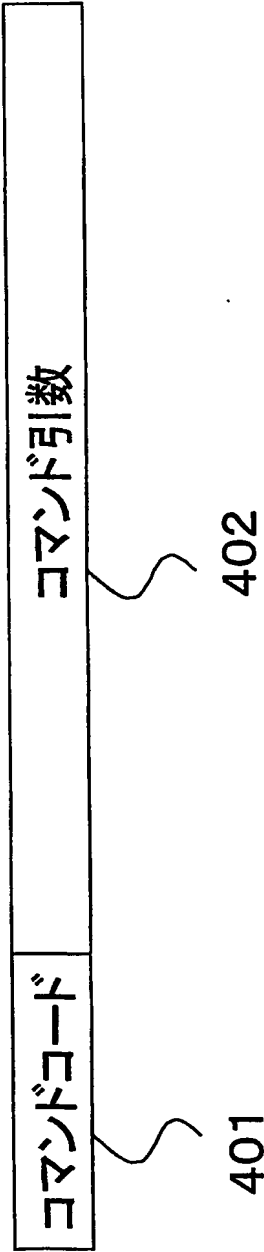
【図 2】



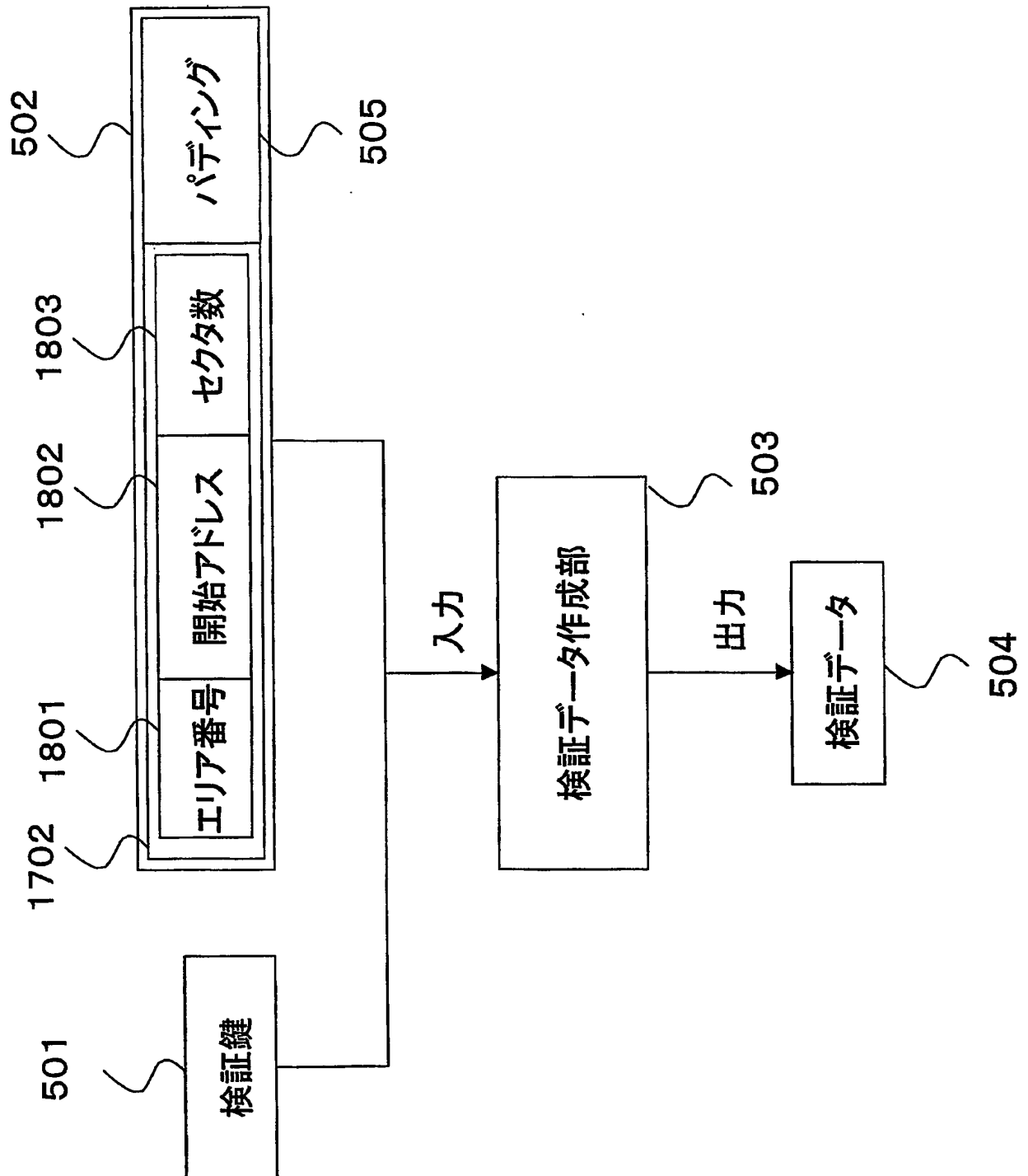
【図 3】



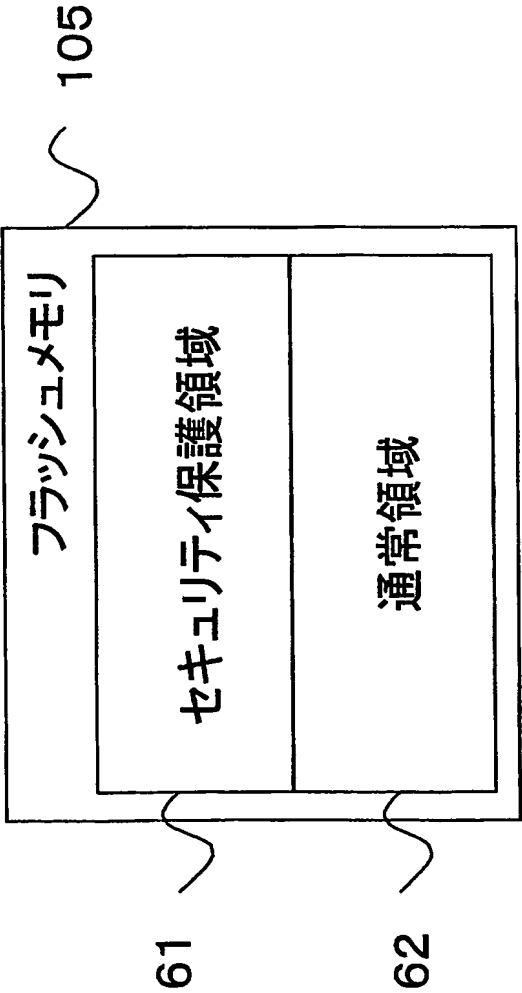
【図 4】



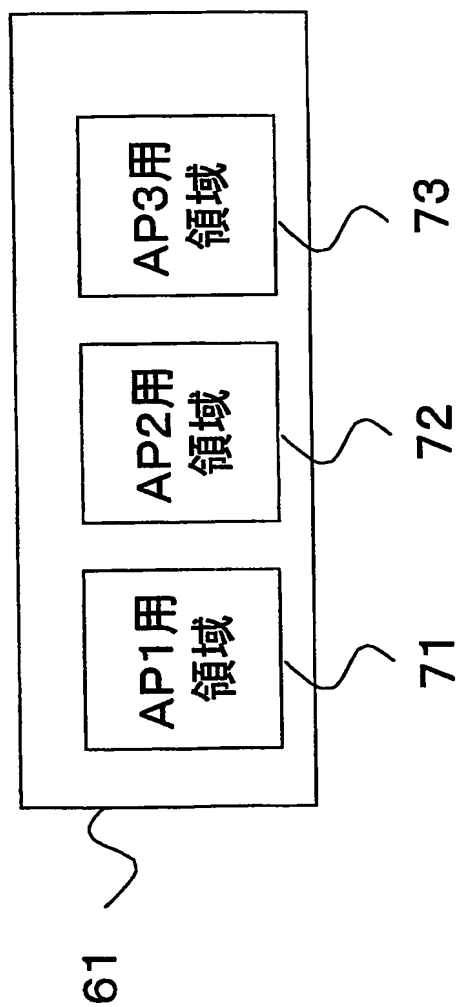
【図 5】



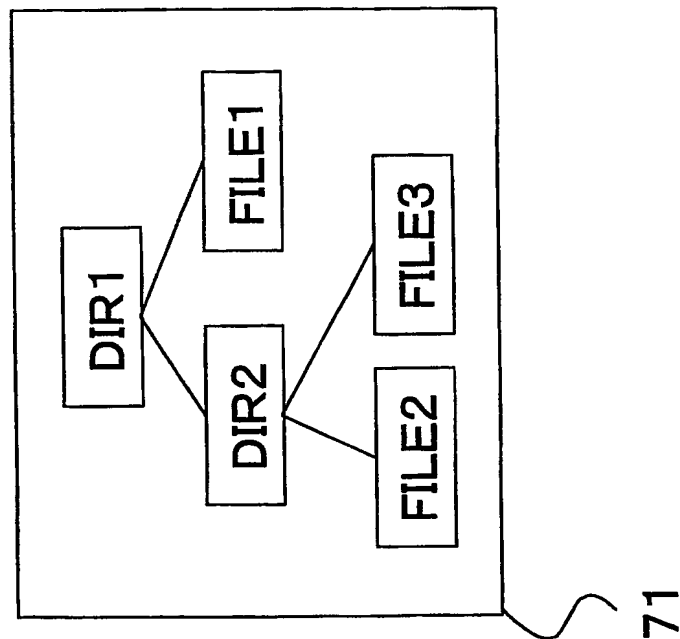
【図 6】



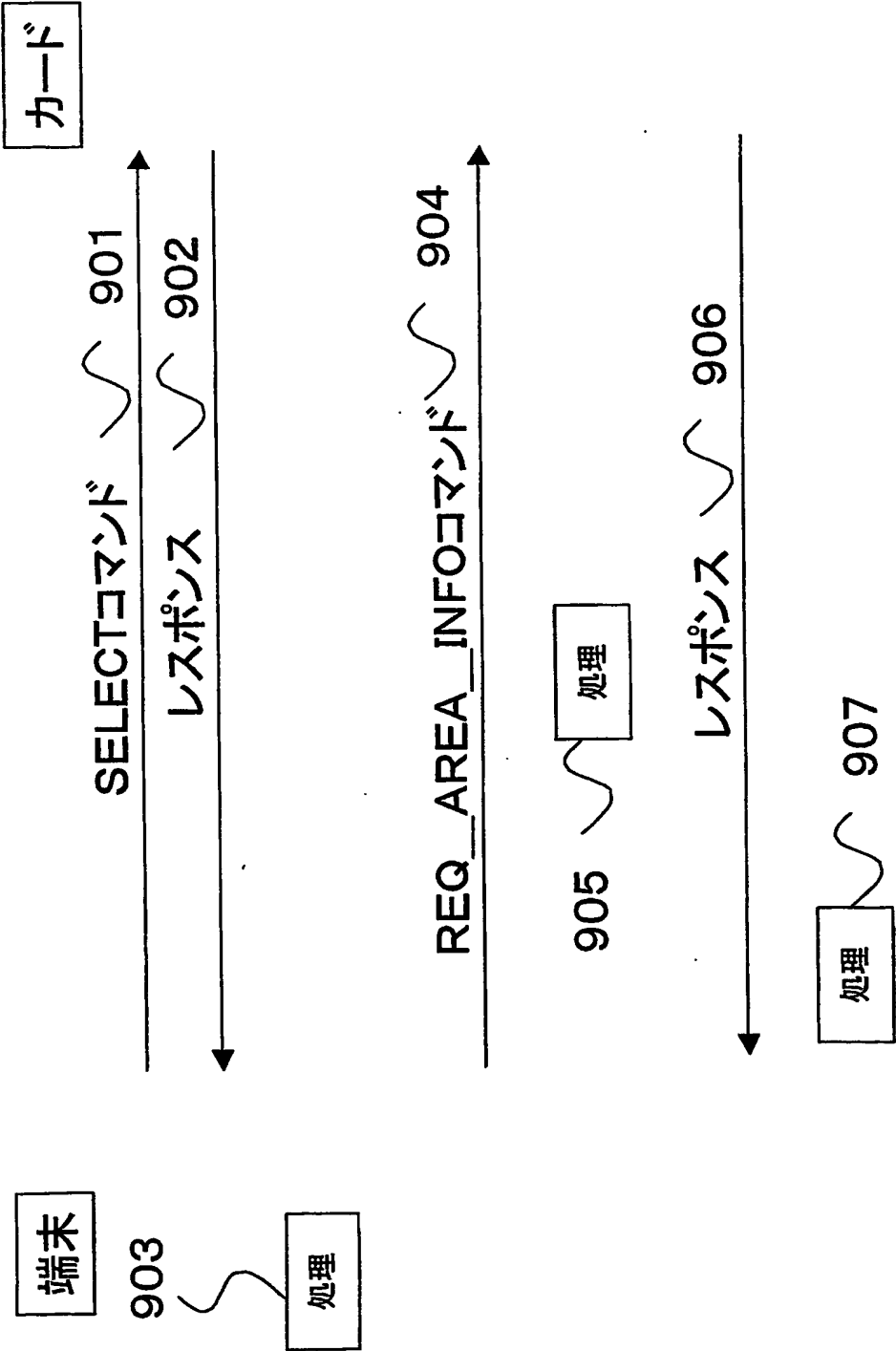
【図 7】



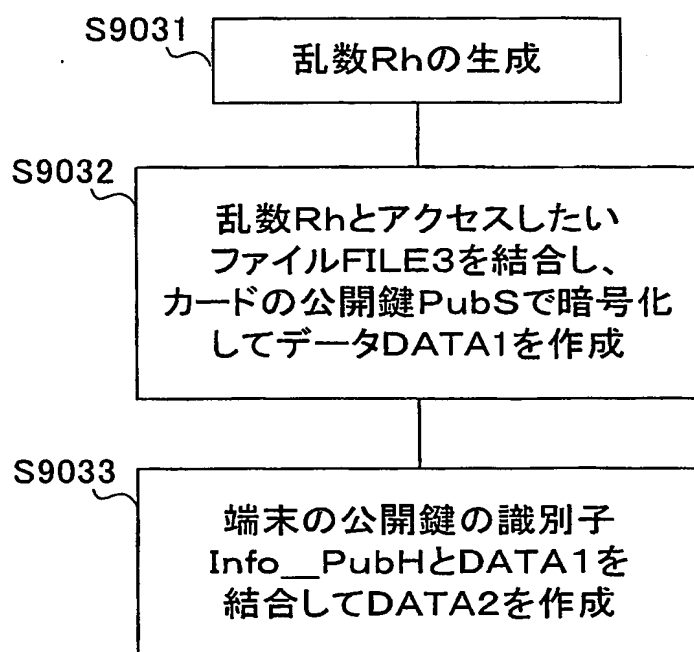
【図 8】



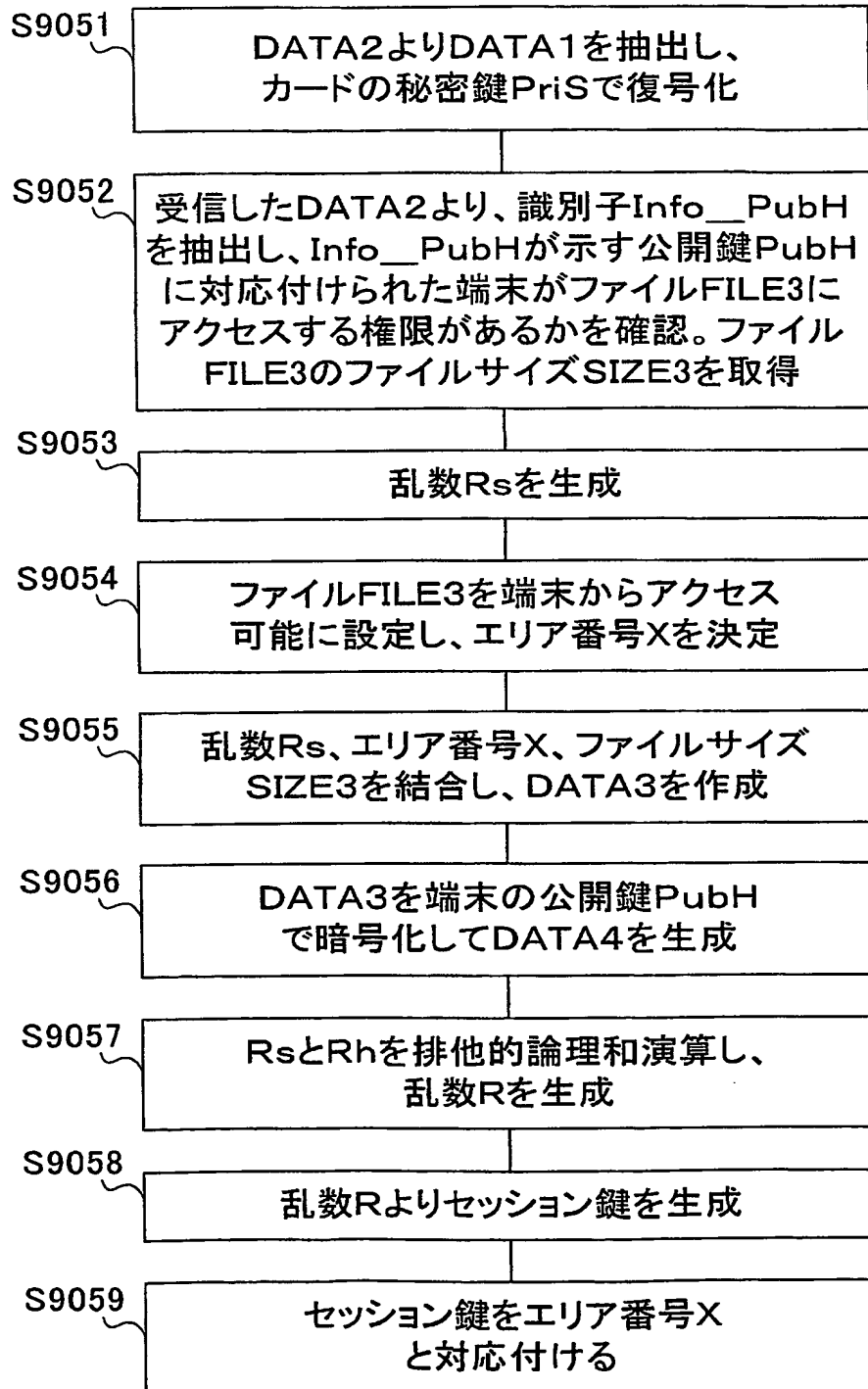
【図 9】



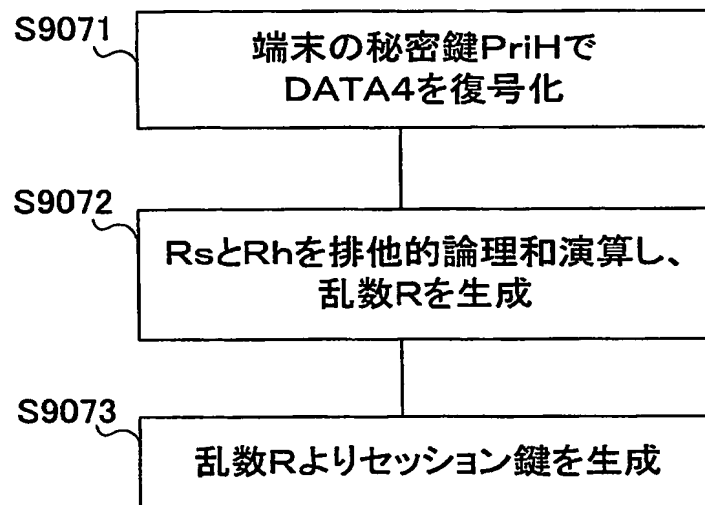
【図10】



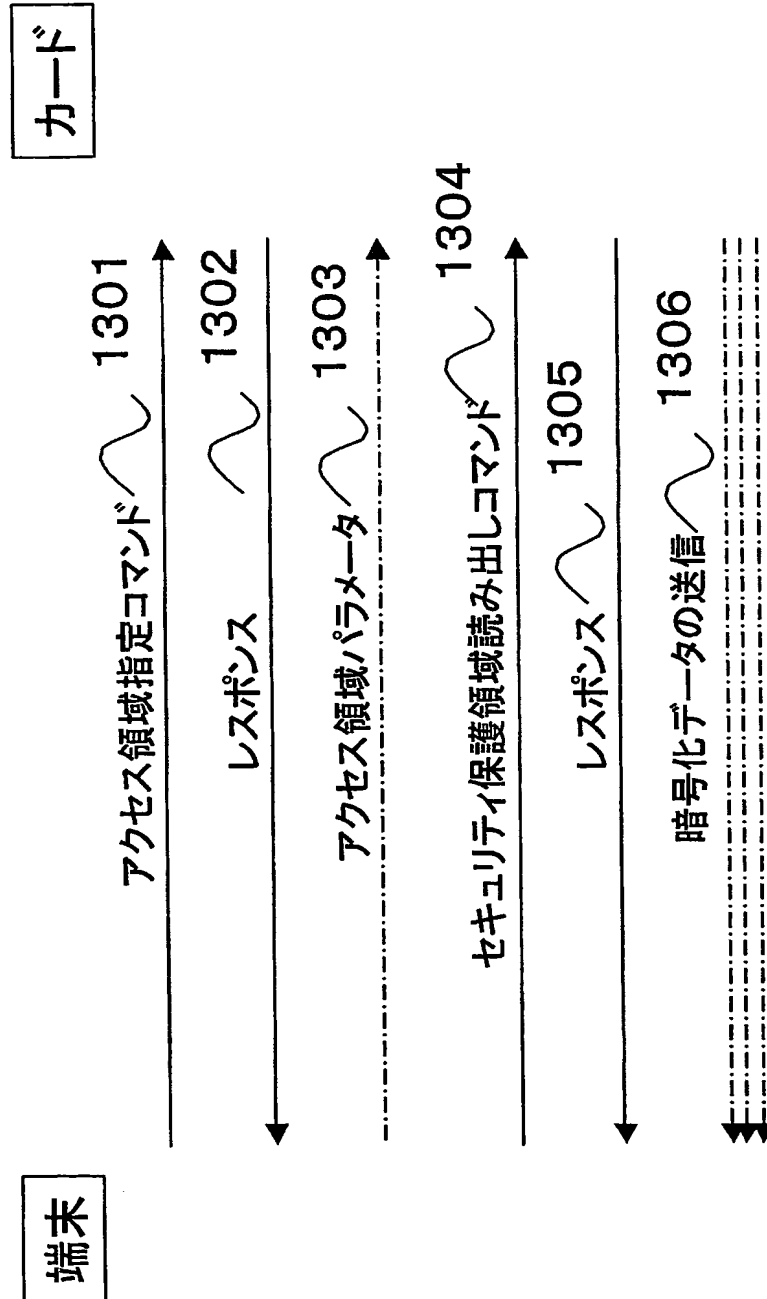
【図 11】



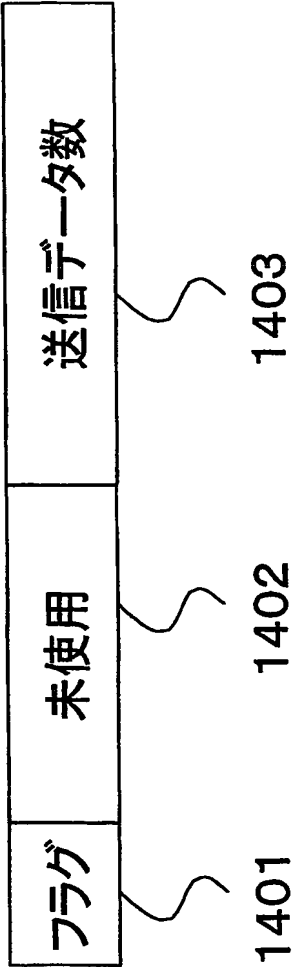
【図 12】



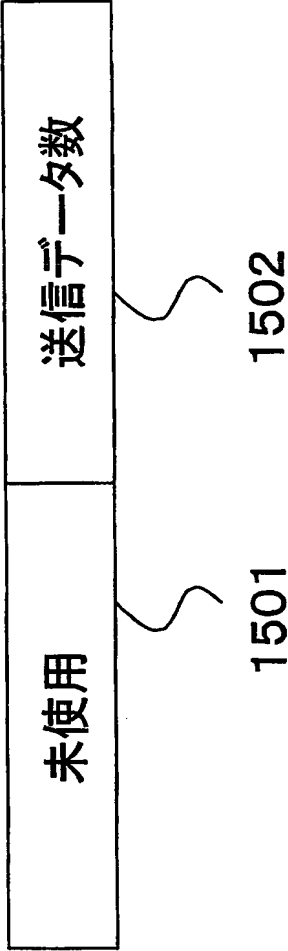
【図 13】



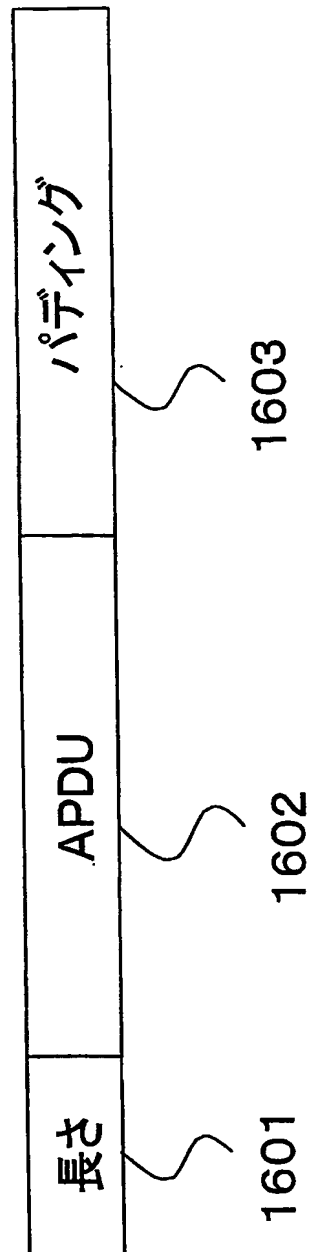
【図 14】



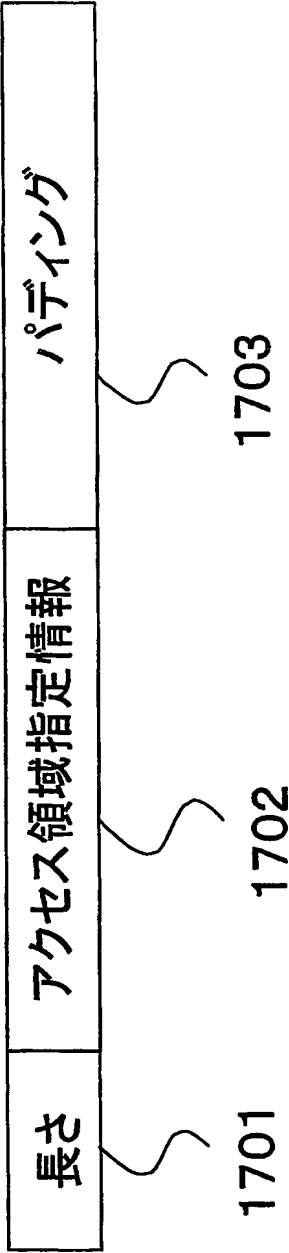
【図 1 5】



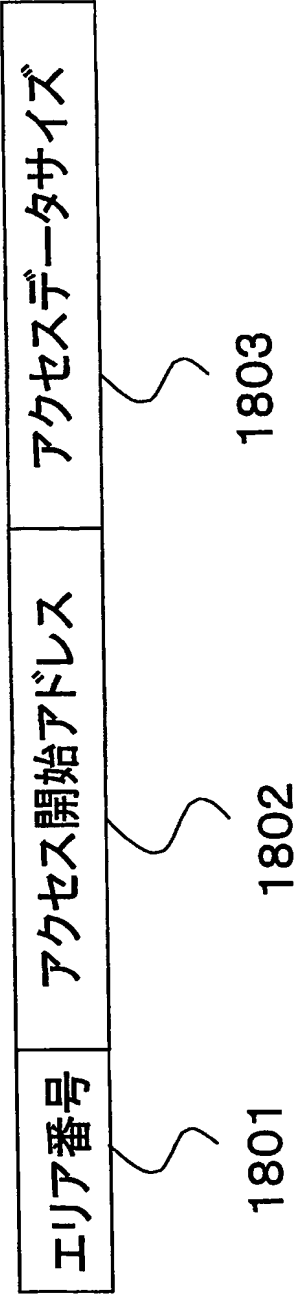
【図 16】



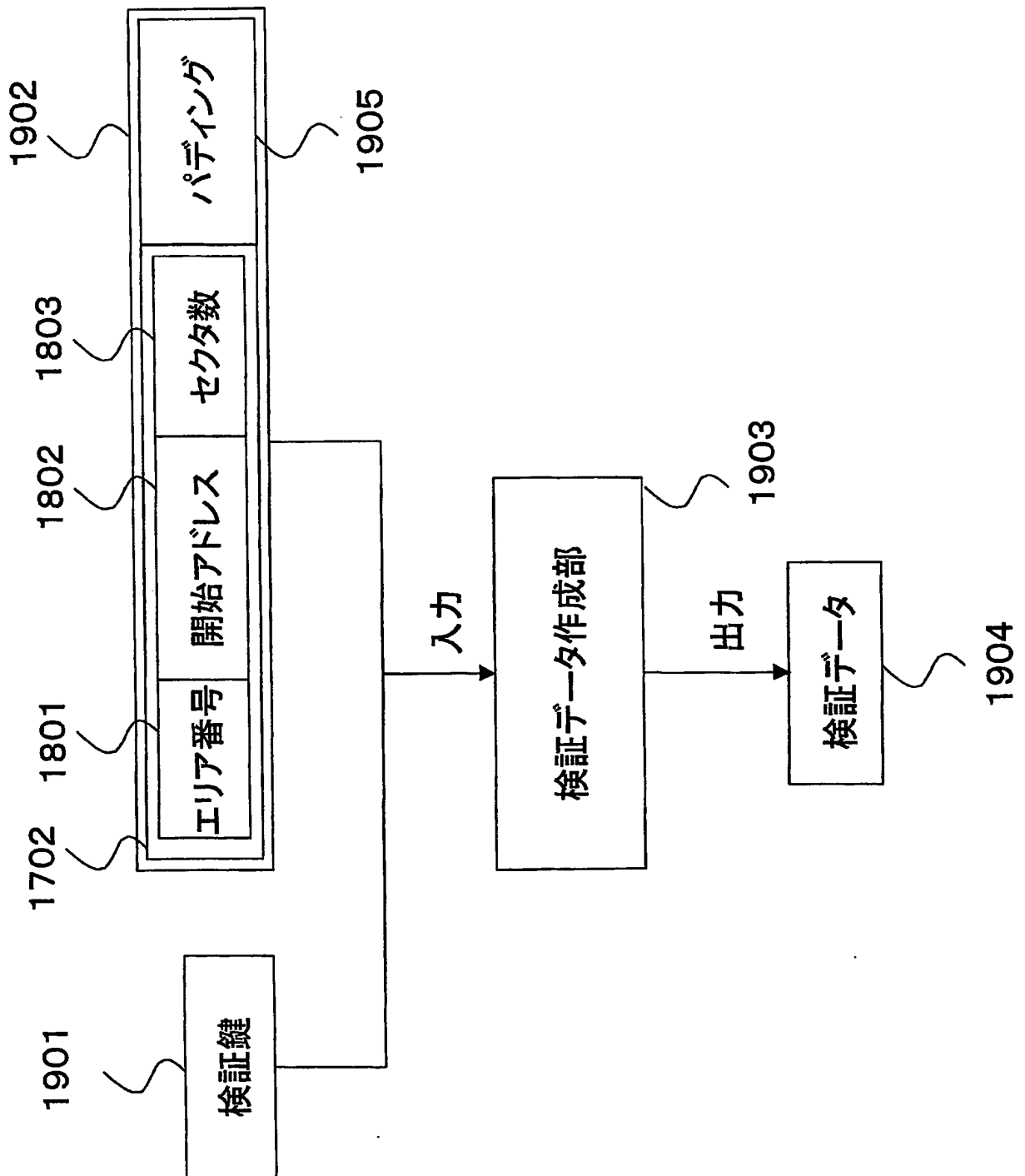
【図 17】



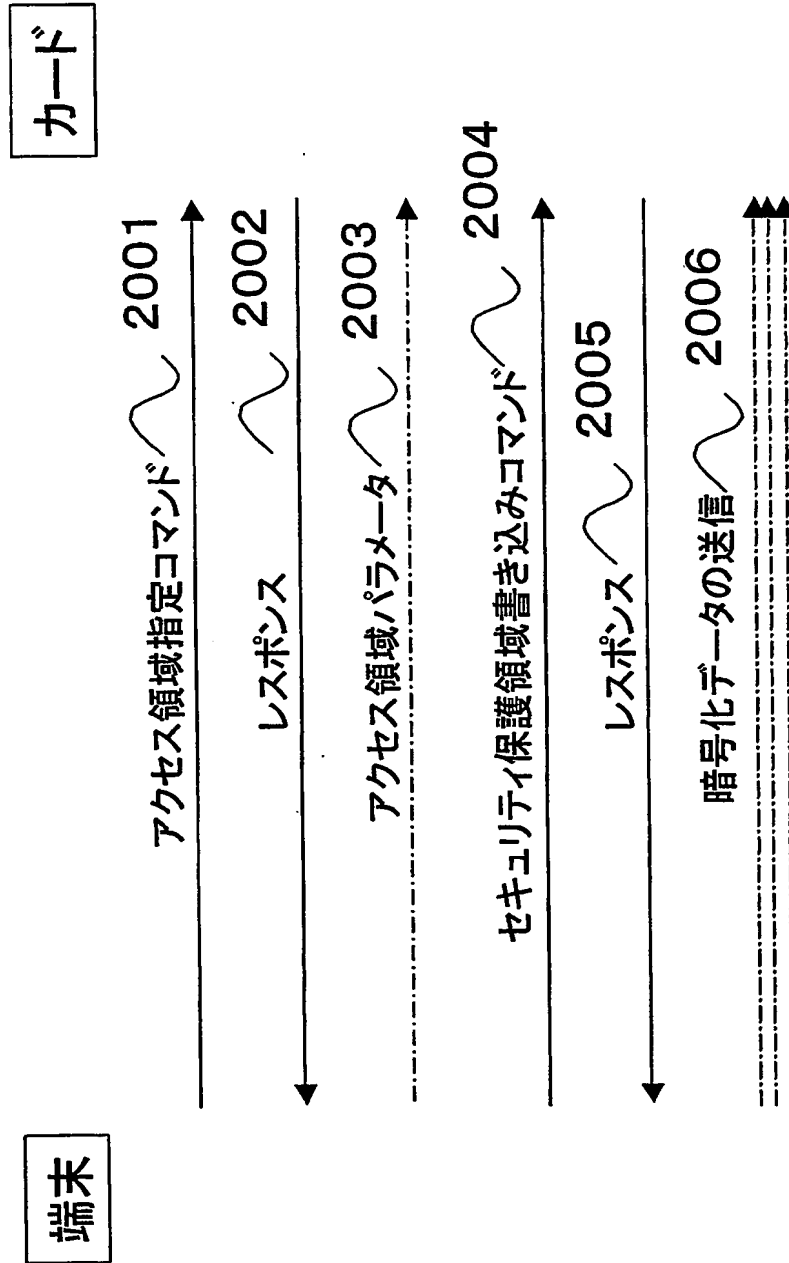
【図 18】



【図 19】



【図 20】



【書類名】 要約書**【要約】**

【課題】 コマンド引数の小さいメモリカードコマンドにおいて、アクセス権限をもった端末を安全に認証可能とする。

【解決手段】 端末からアクセス領域を指定するコマンドと、アクセスを行うコマンドを分離し、アクセスを行うコマンドの引数に端末の検証データを含めて送信することで、アクセス領域を指定するコマンドを発行した端末アプリケーションとアクセスを行うコマンドを発行した端末アプリケーションと、検証用鍵を保有する端末アプリケーションが同一であることが検証可能となる。

【選択図】 図 1

特願 2 0 0 3 - 2 7 5 6 7 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社